

Fig. 1 PRIOR ART

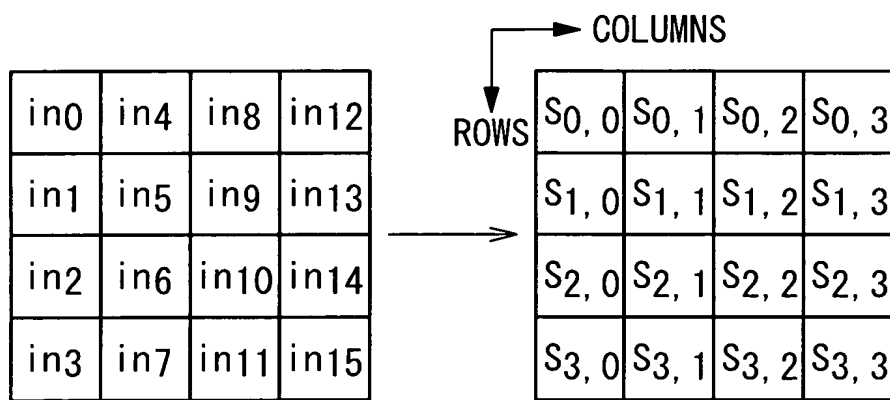


Fig. 2 PRIOR ART

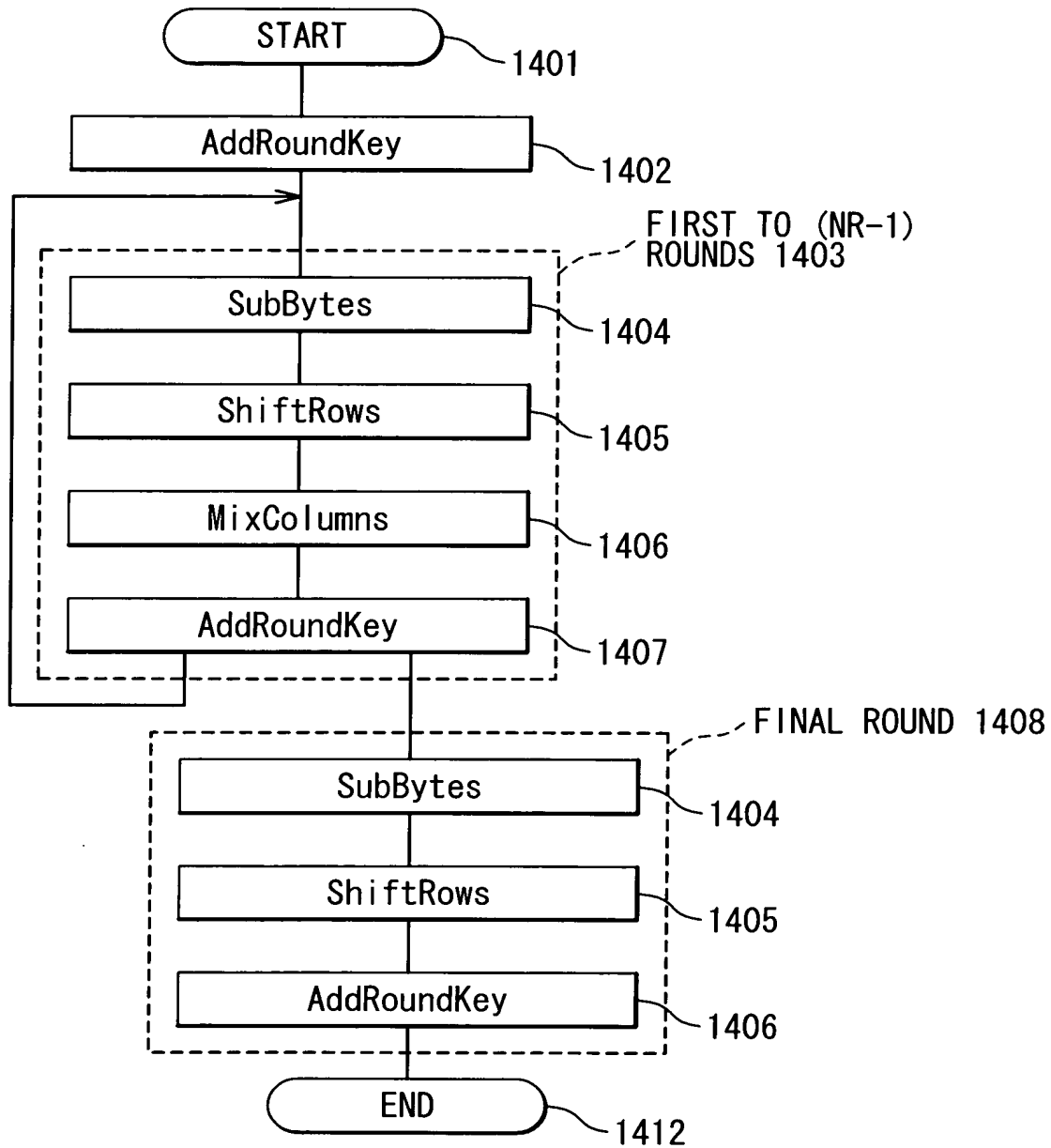


Fig. 3
 PRIOR ART

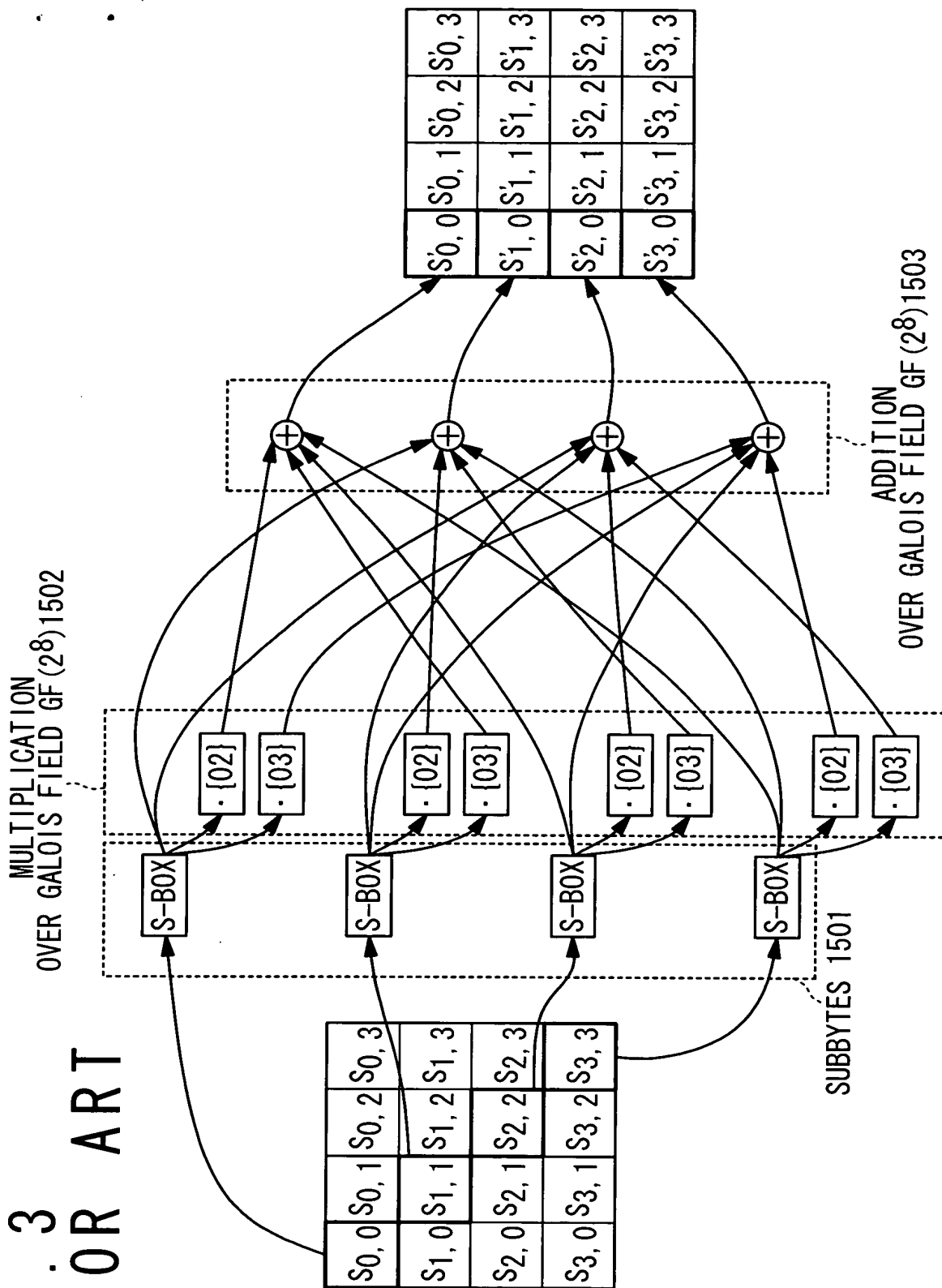


Fig. 4 PRIOR ART

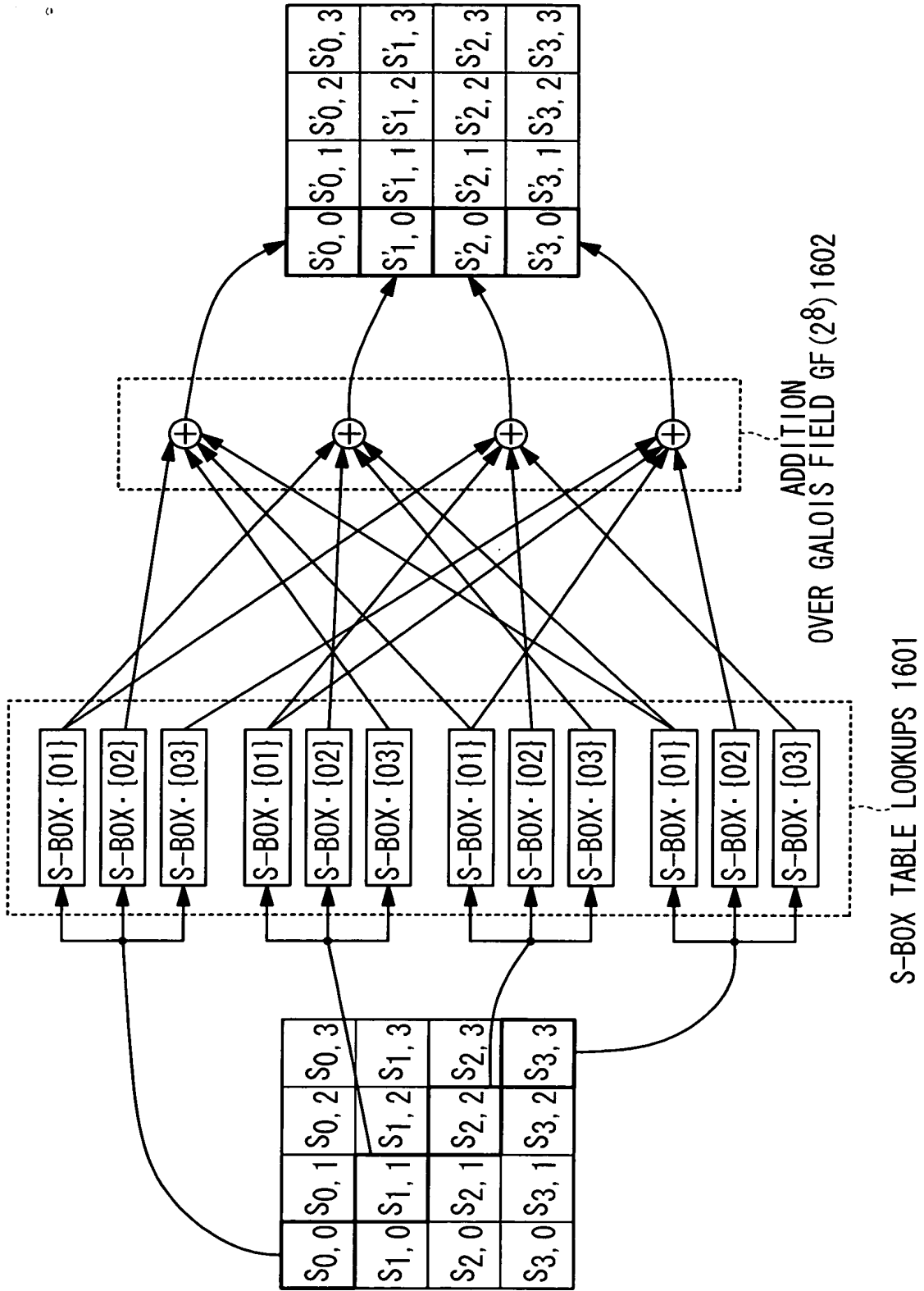


Fig. 5 PRIOR ART

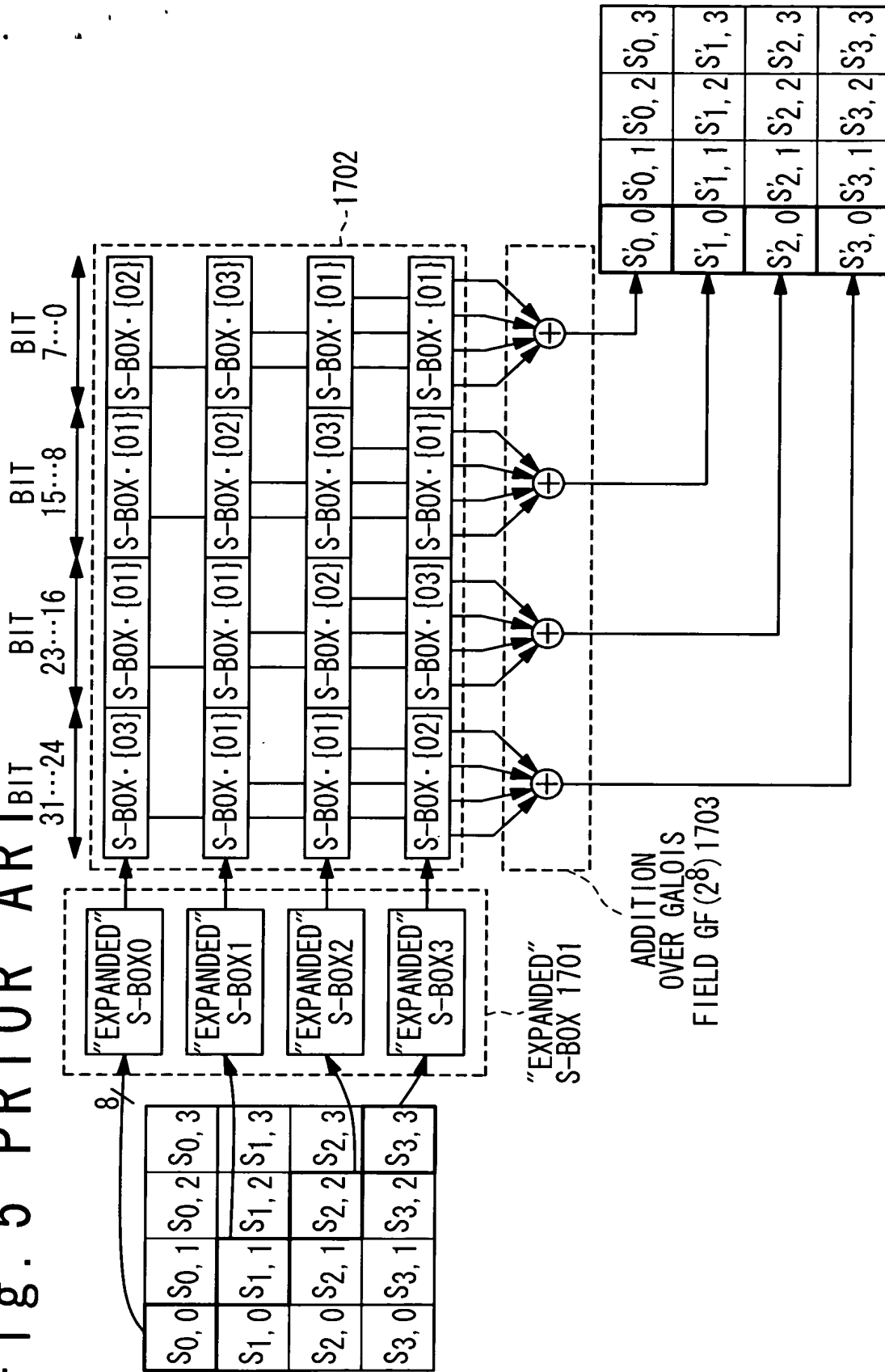


Fig. 6 PRIOR ART

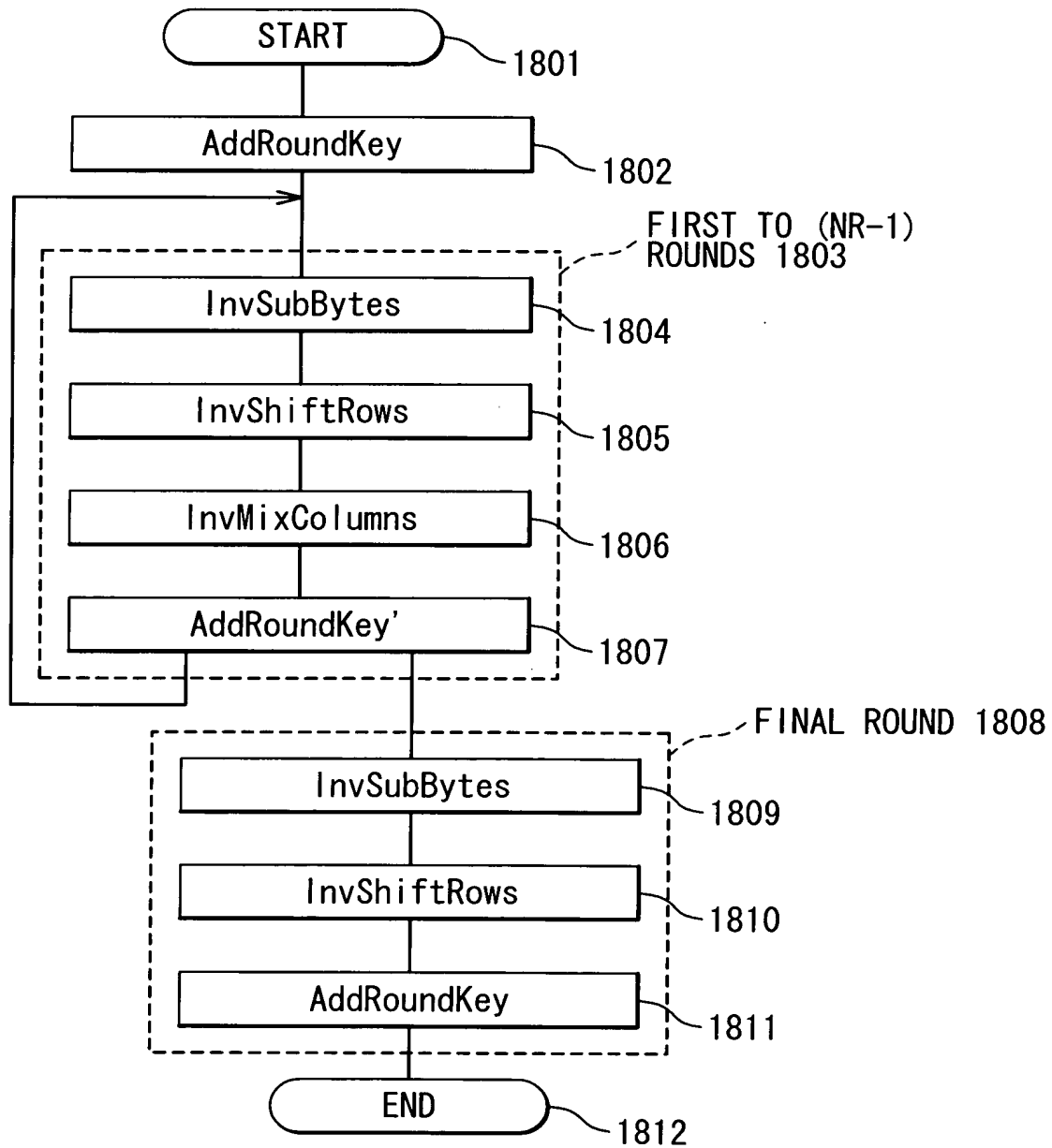


Fig. 7

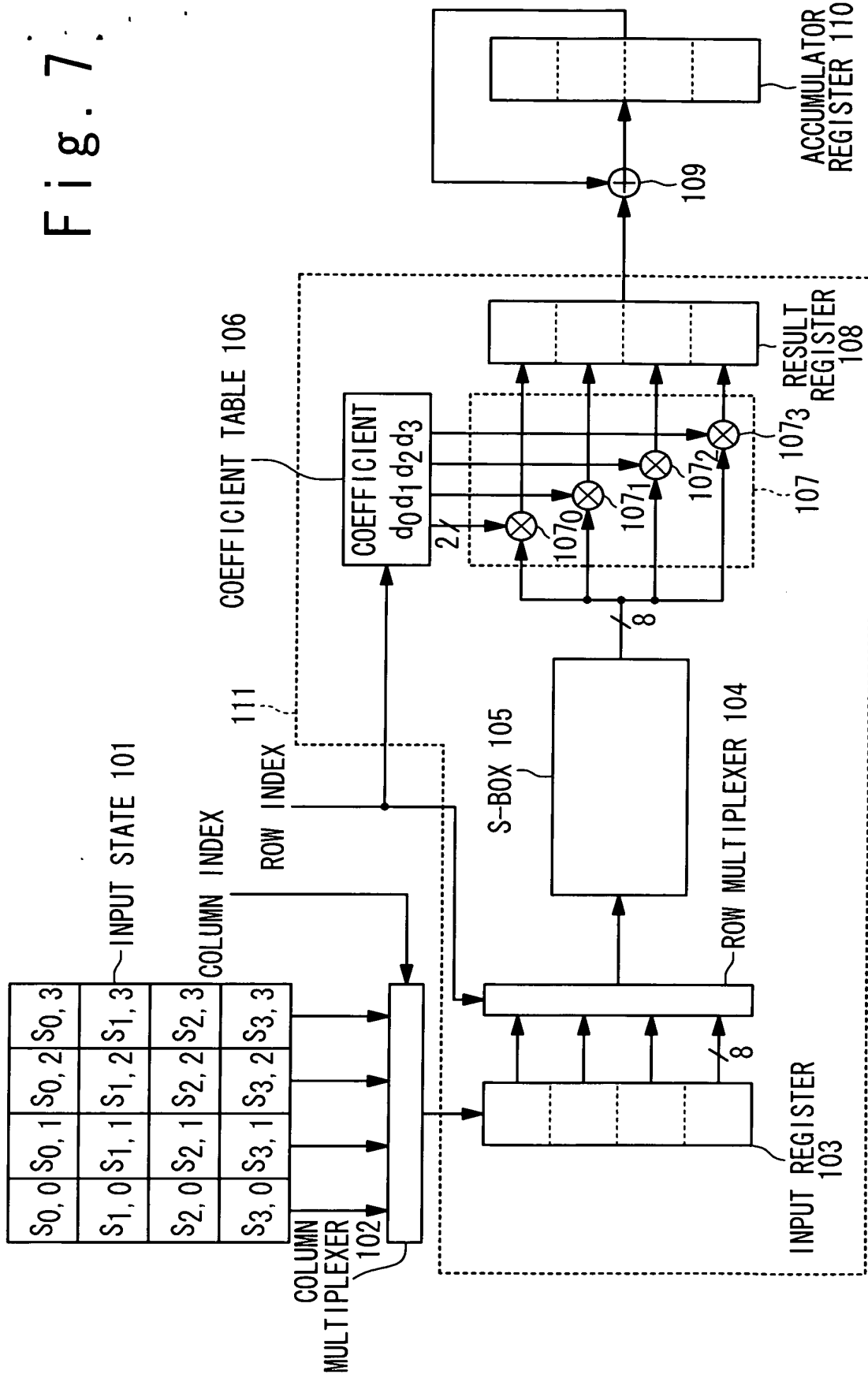


Fig. 8

ROW INDEX	OUTPUT OF COEFFICIENT TABLE			
	d ₃	d ₂	d ₁	d ₀
0	{02}	{01}	{01}	{03}
1	{03}	{02}	{01}	{01}
2	{01}	{03}	{02}	{01}
3	{01}	{01}	{03}	{02}

Fig. 9

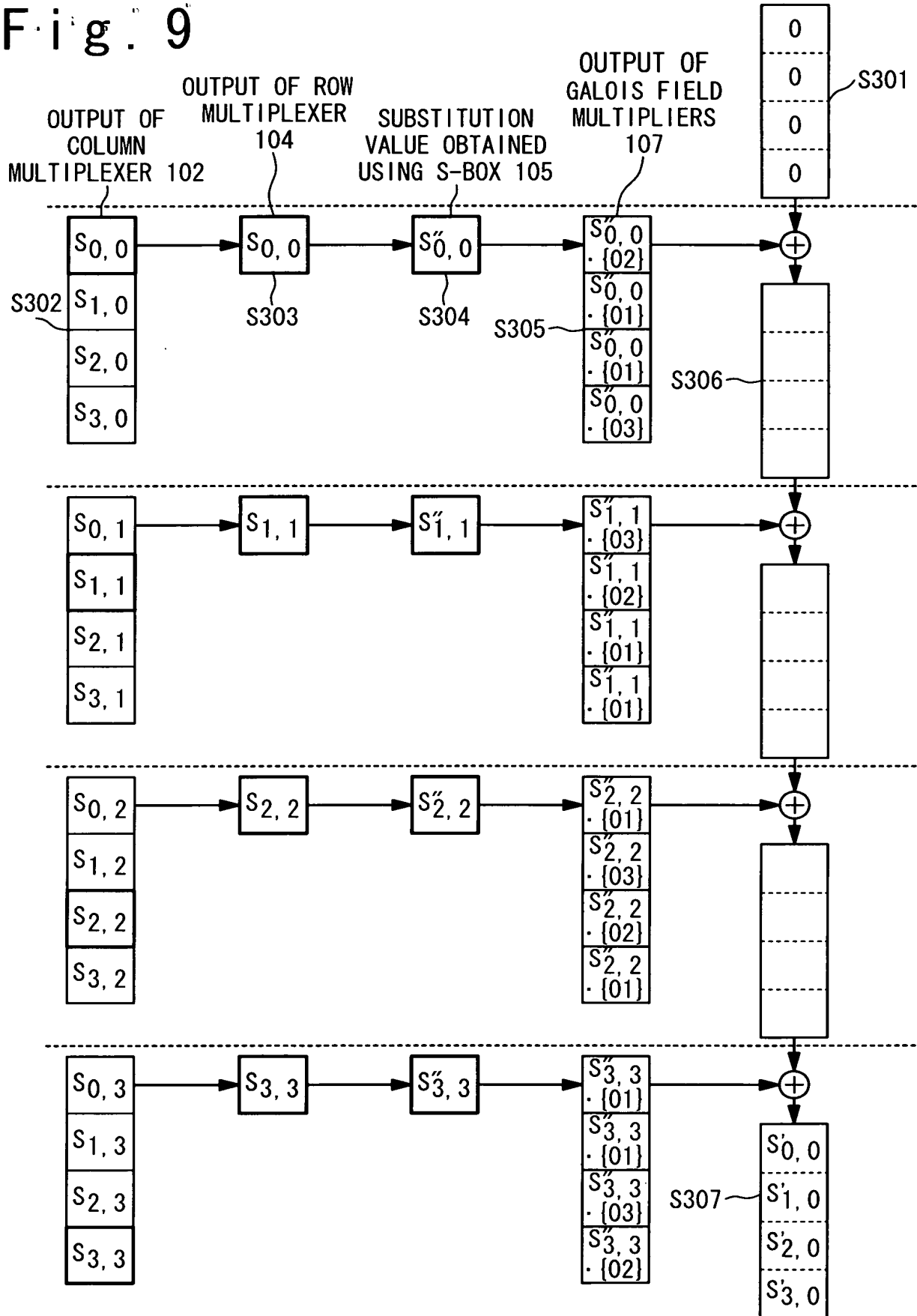
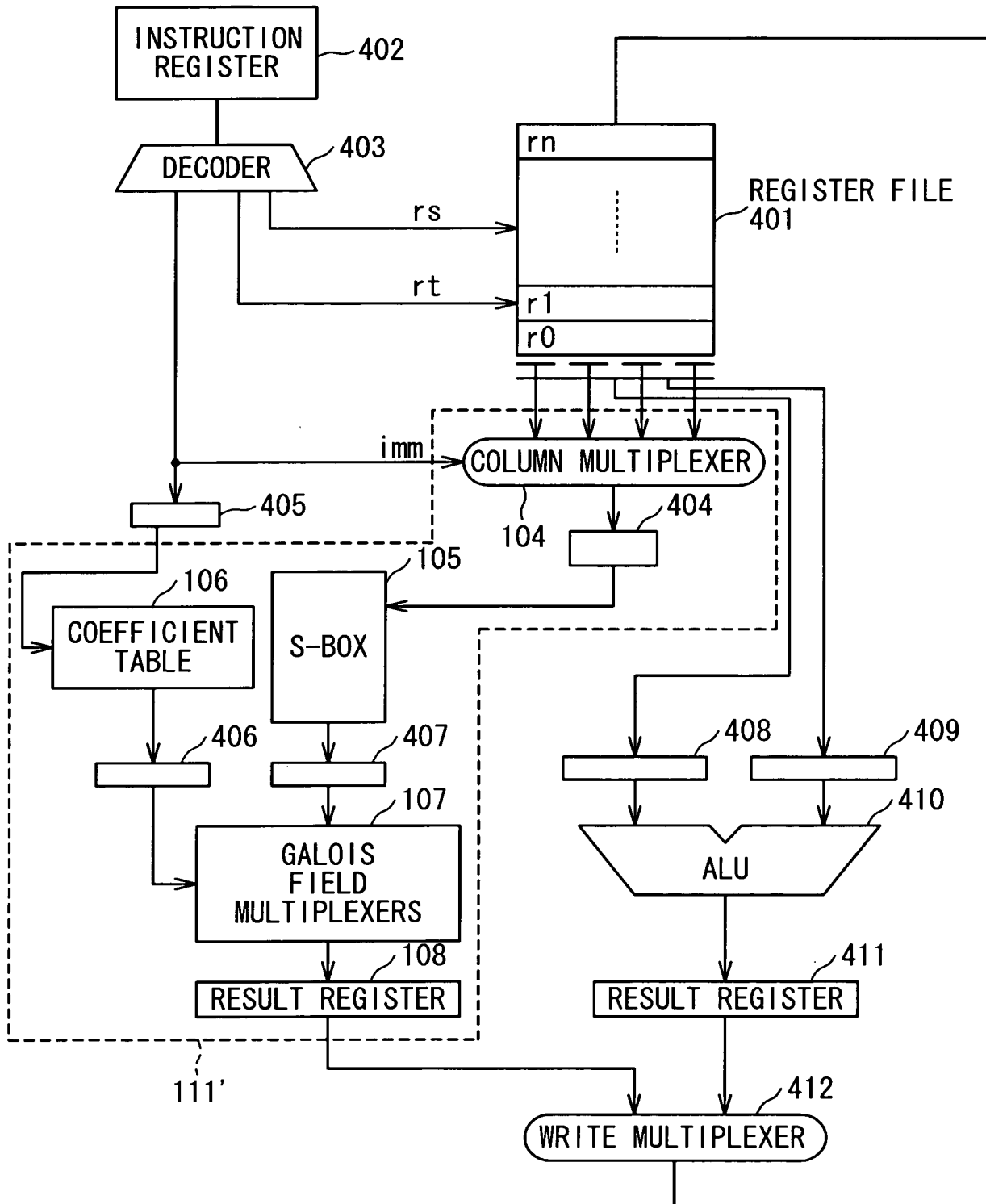
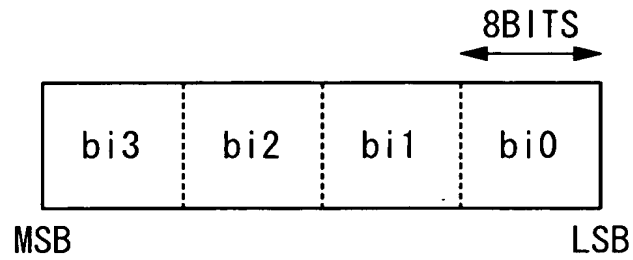


Fig. 10



F i g . 1 1 A



F i g . 1 1 B

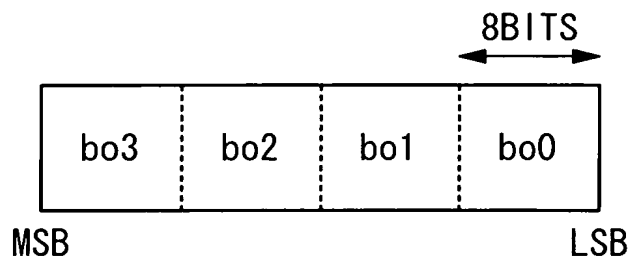


Fig. 12

imm	rt			
	bo3	bo2	bo1	bo0
00	S-B0X(bi0) · {02}	S-B0X(bi0) · {01}	S-B0X(bi0) · {01}	S-B0X(bi0) · {03}
01	S-B0X(bi1) · {03}	S-B0X(bi1) · {02}	S-B0X(bi1) · {01}	S-B0X(bi1) · {01}
02	S-B0X(bi2) · {01}	S-B0X(bi2) · {03}	S-B0X(bi2) · {02}	S-box(bi2) · {01}
03	S-B0X(bi3) · {01}	S-B0X(bi3) · {01}	S-B0X(bi3) · {03}	S-B0X(bi3) · {02}

F i g . 1 3

```
; INPUT:
; r0=[S3,0 S2,0 S1,0 S0,0]
; r1=[S3,1 S2,1 S1,1 S0,1]
; r2=[S3,2 S2,2 S1,2 S0,2]
; r3=[S3,3 S2,3 S1,3 S0,3]
;
; WORK REGISTER:r4
; ACCUMULATOR REGISTER:r5
;
; OUTPUT:
; r5=[S'3,0 S'2,0 S'1,0 S'0,0]
;
AES_SSM r0,r5,0 ; S0,0=r0, bi0
AES_SSM r1,r4,1 ; S1,1=r1, bi1
XOR      r5,r4,r5 ; r5=r5 XOR r4
AES_SSM r2,r4,2 ; S2,2=r2, bi2
XOR      r5,r4,r5 ; r5=r5 XOR r4
AES_SSM r3,r4,3 ; S3,3=r3, bi3
XOR      r5,r4,r5 ; r5=r5 XOR r4
```

Fig. 14

ROW INDEX	OUTPUT OF COEFFICIENT TABLE			
	d ₃	d ₂	d ₁	d ₀
0	{0e}	{09}	{0d}	{0b}
1	{0b}	{0e}	{09}	{0d}
2	{0d}	{0b}	{0e}	{09}
3	{09}	{0d}	{0b}	{0e}

Fig. 15

imm	rt			
	bo3	bo2	bo1	bo0
00	INVS-B0X (bi0) · {0e}	INVS-B0X (bi0) · {09}	INVS-B0X (bi0) · {0d}	INVS-B0X (bi0) · {0b}
01	INVS-B0X (bi1) · {0b}	INVS-B0X (bi1) · {0e}	InvS-box (bi0) · {09}	INVS-B0X (bi1) · {0d}
02	INVS-B0X (bi2) · {0d}	INVS-B0X (bi2) · {0b}	INVS-B0X (bi2) · {0e}	INVS-B0X (bi2) · {09}
03	InvS-box (bi3) · {09}	InvS-box (bi3) · {0d}	INVS-B0X (bi3) · {0b}	INVS-B0X (bi3) · {0e}

Fig. 16

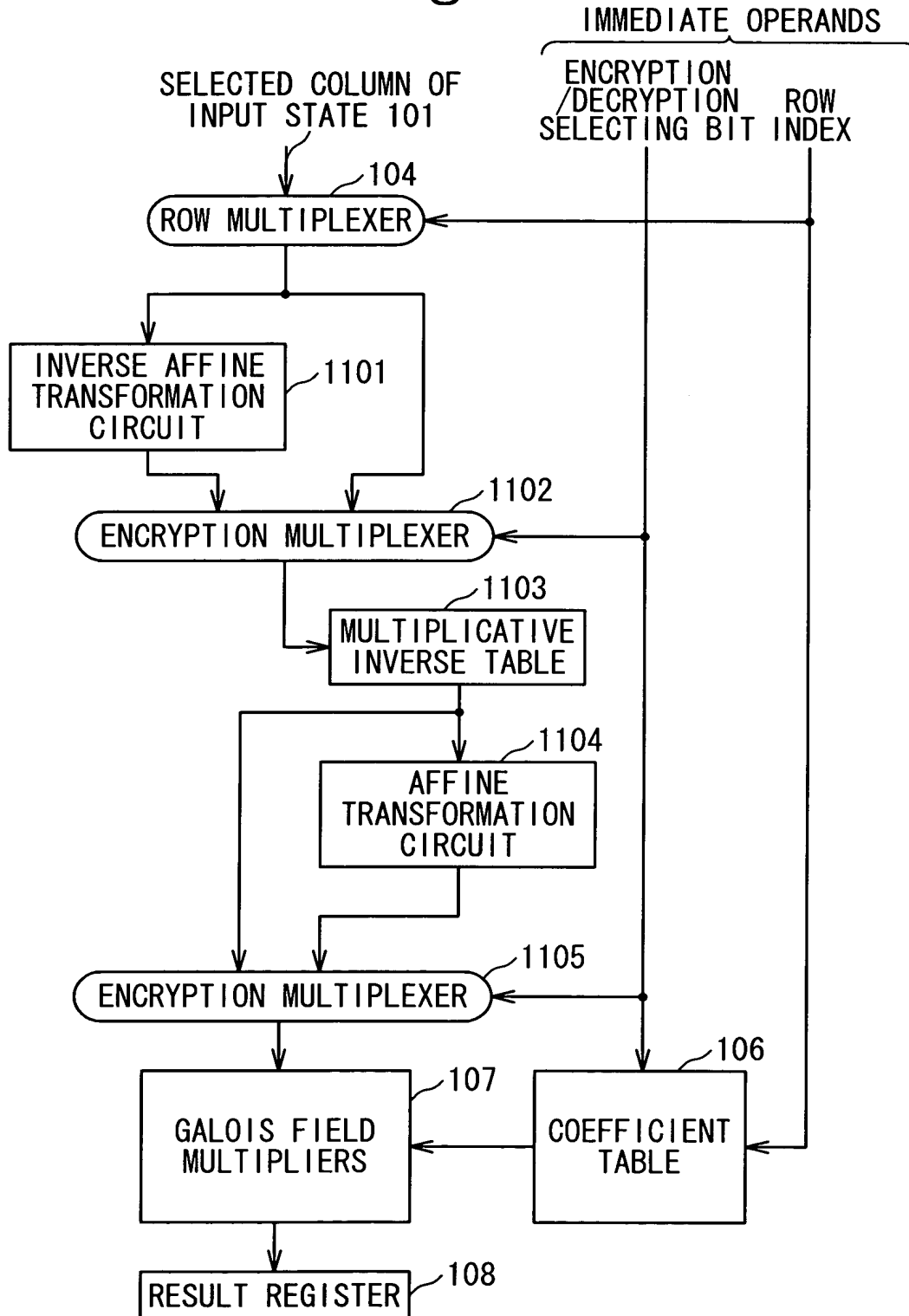


Fig. 17

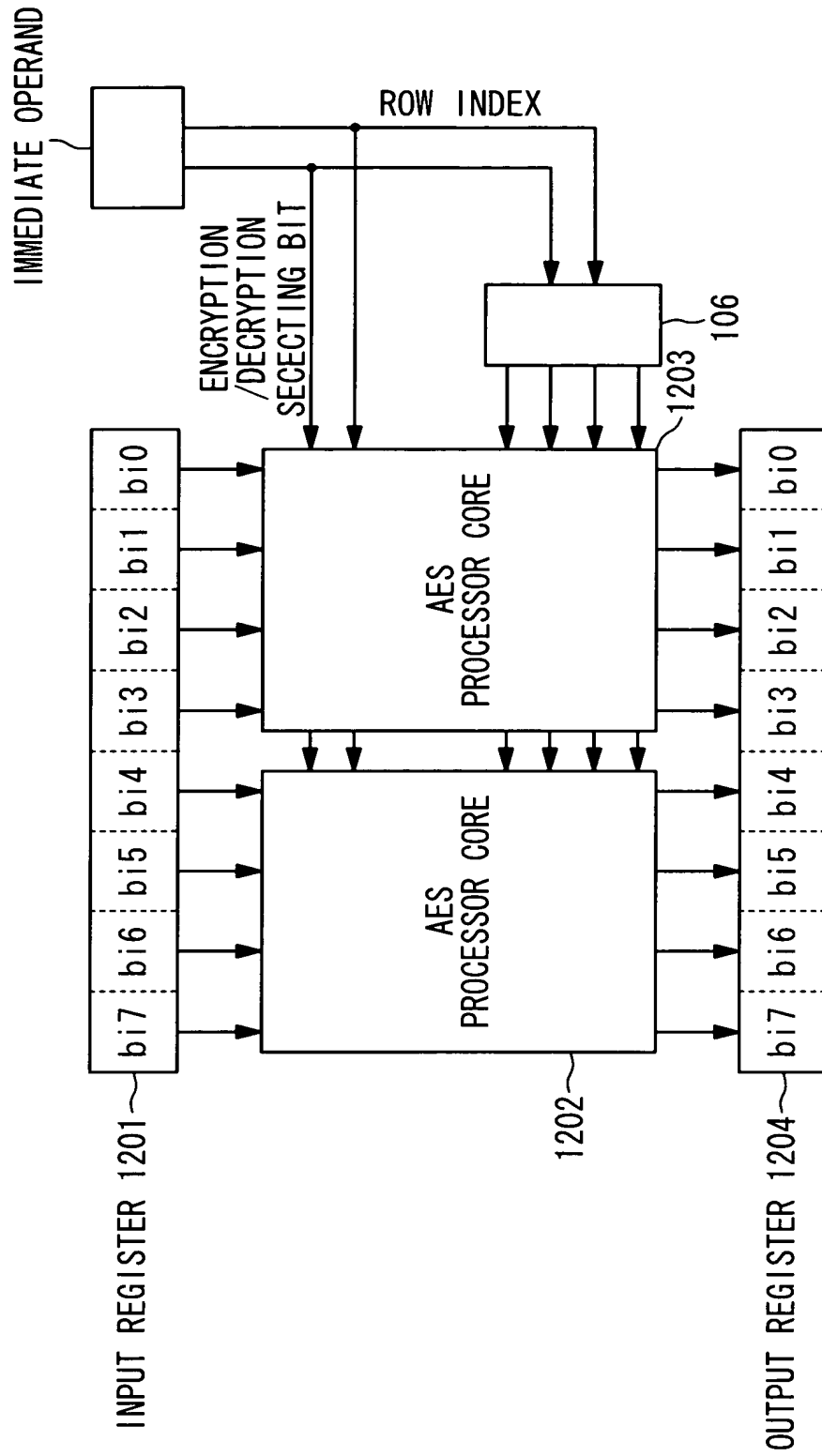
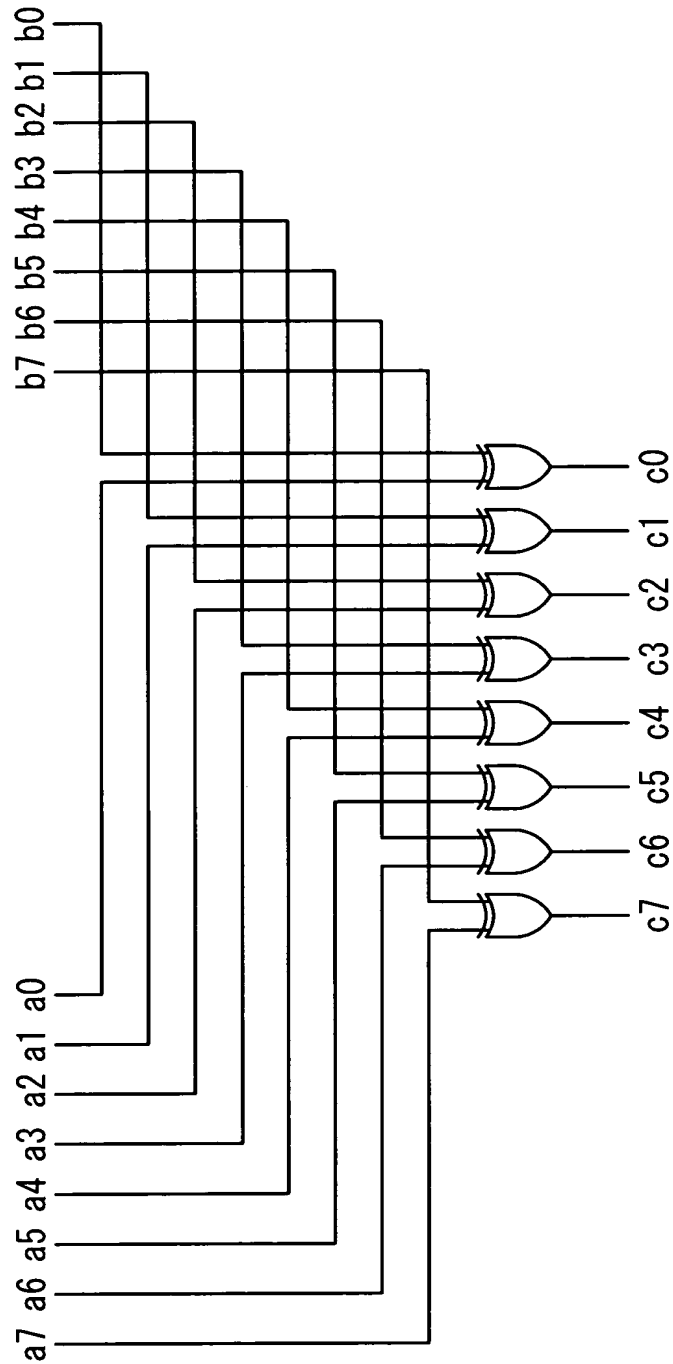


Fig. 18



F i g . 1 9

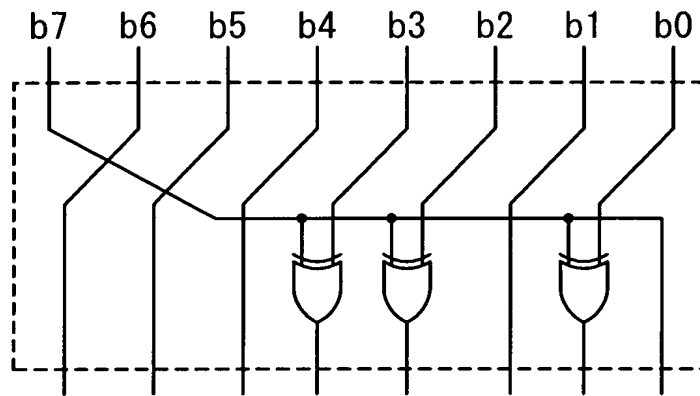
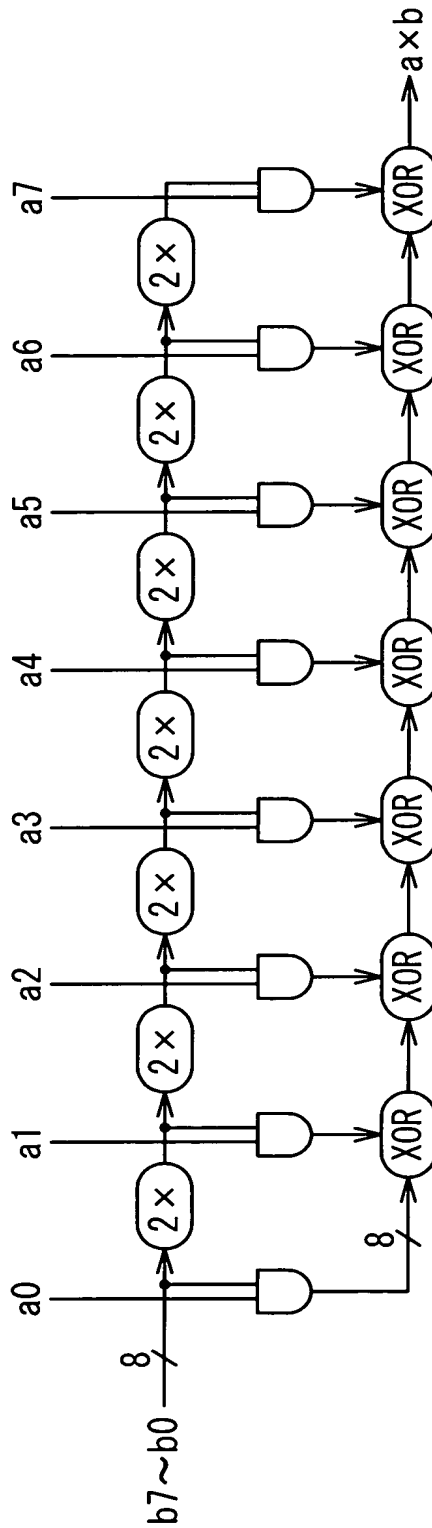


Fig. 20



F i g . 21

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
f	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

F i g . 2 2

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
f	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

F i g . 2 3

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
f	0	00	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
	1	74	b4	aa	4b	99	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2
	2	3a	6e	5a	f1	55	4d	a8	c9	c1	0a	98	15	30	44	a2	c2
	3	2c	45	92	6c	f3	39	66	42	f2	35	20	6f	77	bb	59	19
	4	1d	fe	37	67	2d	31	f5	69	a7	64	ab	13	54	25	e9	09
	5	ed	5c	05	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17
	6	16	5e	af	d3	49	a6	36	43	f4	47	91	df	33	93	21	3b
	7	79	b7	97	85	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82
	8	83	7e	7f	80	96	73	be	56	9b	9e	95	d9	f7	02	b9	a4
	9	de	6a	32	6d	d8	8a	84	72	2a	14	9f	88	f9	dc	89	9a
	a	fb	7c	2e	c3	8f	b8	65	48	26	c8	12	4a	ce	e7	d2	62
	b	0c	e0	1f	ef	11	75	78	71	a5	8e	76	3d	bd	bc	86	57
	c	0b	28	2f	a3	da	d4	e4	0f	a9	27	53	04	1b	fc	ac	e6
	d	7a	07	ae	63	c5	db	e2	ea	94	8b	c4	d5	9d	f8	90	6b
	e	b1	0d	d6	eb	c6	0e	cf	ad	08	4e	d7	e3	5d	50	1e	b3
	f	5b	23	38	34	68	46	03	8c	dd	9c	7d	a0	cd	1a	41	1c